Capítulo 12. Instalación y uso

12.1 Introducción

Esta sección presenta un completo manual para la instalación del sistema de firma digital XML. Tras la instalación, se describe cómo ejecutar cada unos de los subsistemas de firma y validación que componen la aplicación así como los posibles parámetros que se pueden indicar.

El sistema de firma digital XML desarrollado es totalmente independiente de la plataforma en la que se implante ya que está formado por código cien por cien Java. Para ello, sólo precisa tener instalado la herramienta **JavaTM 2 SDK, Standard Edition Version 1.4.2** para aportar todas las funcionalidades necesarias para poder compilar y ejecutar la aplicación Java. Así contará con la máquina virtual Java, APIS Java para realizar operaciones específicas y herramientas de compilación.

12.2 Manual de instalación

El proceso de instalación del sistema resulta bastante sencillo, basta con incluir las librerías de las que uso el sistema en el JDK y compilar el código fuente de los subsistemas de firma y validación.

12.2.1 Librerías utilizadas

Las librerías que deben incluirse para ejecutar la aplicación son las siguientes:

- **jsr173_1.0_ri.jar** y **jsr173_1.0_api.jar.** Contienen la implementación del analizador XML StAX utilizado para leer los documentos XML y generar la salida firmada.
- **dtdparser121.jar.** Esta librería complementa el funcionamiento del analizador XML permitiendo la interpretación de la información contenida en la declaración DTD de un documento XML.
- **commons-codec-1.4-dev.jar.** Implementación del método de codificación Base64 necesario para la representación de los valores de resumen y firma.

Estas librerías deben ubicarse en los directorios del JDK:

- C:\jdk1.x\jre\lib\ext.

- C:\ArchivosdePrograma\Java\jre\lib\ext.

Una vez incluidas las librerías en estos directorios se puede compilar y ejecutar la aplicación como se describe en las siguientes secciones.

12.2.2 Compilación del código fuente

El sistema se presenta en un paquete denominado Firma que contiene los ficheros con las clases que albergan los métodos *main()* de los subsistemas de firma y validación. Estos ficheros son:

- Firmar.java
- Validar.java

El directorio Firma contiene además los paquetes donde se encuentra el API de firma y que son los siguientes:

- castanedo.xml.crypto.
- castanedo.xml.crypto.dsig
- castanedo.xml.crypto.dsig.stax
- castanedo.xml.crypto.dsig.keyinfo

Para compilar el susbistema de firma debe ejecutarse la siguiente orden desde la línea de comandos:

> *javac Firmar.java*

Análogamente, para compilar el código del subsistema de validación se ejecuta desde la línea de comandos:

> *javac Validar.java*

Al compilar estas clases también se compila el código del API de firma por lo que desde este instante es posible ejecutar la aplicación.

12.3 Ejecución del subsistema de firma

El subsistema de firma permite generar documentos XML firmados en cualquiera de los tres formatos ENVELOPED, ENVELOPING y DETACHED.

Los parámetros de entrada que deben especificarse para ejecutar la aplicación son los siguientes:

- Nombre del recurso XML que se desea firmar.
- Nombre que se desea para el documento firmado.
- Formato de la firma. Admite tres posibles valores enveloped, enveloping y detached.
- Valor del atributo id del elemento que se desea firmar. Este parámetro es opcional si se ha especificado que el formato de salida sea enveloped.

Teniendo en cuenta estos parámetros de entrada, para ejecutar el subsistema de firma se debe ejecutar alguna de estas órdenes desde la línea de comandos según el formato de firma:

>java Firmar docentrada.xml salidaenveloped.xml enveloped

Si se desea que el formato de salida sea *enveloping* se debe ejecutar el comando:

>java Firmar docentrada.xml salidaenveloping.xml enveloping idelemento

Por último para generar la firma en formato *detached* se ejecuta:

>java Firmar docentrada.xml salidadetached.xml detached idelemento

Tras la ejecución de alguno de estos comandos se puede comprobar que se ha generado el documento firmado con el nombre especificado como parámetro de entrada.

12.4 Ejecución del subsistema de validación

El subsistema de validación permite verificar un documento firmado, comprobando la integridad de la información y autenticando al firmante. Para ejecutar esta aplicación sólo es necesario especificar como parámetro de entrada el nombre del documento firmado que se pretende validar por lo que basta con ejecutar el siguente comando:

>java Validar docfirmado.xml

Ante la ejecución de este comando el sistema puede presentar los siguientes mensajes:

- *"La referencia no es válida"* Indica que el valor del resumen que contiene la firma no se corresponde con la información firmada por lo que no se puede garantizar la integridad de dicha información.
- *"La firma no es válida"* En este caso el valor del resumen es correcto, sin embargo el valor de la firma no coincide con el calculado en el proceso de

validación por lo que no se puede autentificar al firmante.

- *“La firma es válida”* Se garantiza la integridad de la información firmada y la autenticidad del firmante, por lo que también se elimina la posibilidad de repudio por parte del firmante ya que el documento se ha firmado con su clave privada.